"Pandemia aumenta crimes de usurpação de identidade e roubo do email"

rr.sapo.pt/2020/04/16/pais/pandemia-aumenta-crimes-de-usurpacao-de-identidade-e-roubo-do-email/noticia/189473

April 16, 2020

Bruno Castro, presidente da Visionware, perito em cibercrime, diz que é difícil chegar ao autor ou organização que fez o ataque.

A pandemia de Covid-19 abriu portas a um esquema de trabalho diferente, o teletrabalho, e abriu portas também a uma maior fragilidade da segurança das empresas e particulares. A opinião é expressa à **Renascença** por Bruno Castro, perito em cibercrime e presidente da Visionware.

"O mundo mudou e nunca mais será o mesmo. Todos temos de usar o computador e internet", afirma Bruno Castro, aludindo ao caso da EDP, que foi vítima disso.

No passado dia 13 de Abril, a empresa deu conta de um ataque Ransonmware. O método não é novo, é de resto vulgar e deixa as empresas "entre a espada e a parede".

"O resgate é pedido em função da dimensão da empresa ou da sensibilidade dos dados roubados", explica Bruno Castro, acrescentando que "é isso que mede a verba que é pedida como contrapartida para tudo regressar à aparente normalidade".

"Neste tipo de ataque tem-se acesso à infraestrutura da organização, a dados confidenciais, incripta-se os dados com uma chave digital e pede-se resgate para que a empresa tenha acesso de novo a esses mesmos dados", explica.

A recomendação, diz, é que "nunca se pague o resgate". Primeiro, porque se está a alimentar uma rede criminosa e, em segundo, porque não há garantia da empresa voltar a ter tudo de volta.

"Nada garante que se tem os dados de novo. Mesmo que isso aconteça,, pontualmente, as empresas recebem a chave de volta e o negocio é retomado, mas não há garantia de que não haja novos ataques", diz Castro, lembrando que os criminosos ficam sempre com a informação que roubam.

"Há uma falsa sensação de recuperação de segurança porque, depois, os criminosos podem sempre estudar os emails e ficheiros e fazer novo tipo de chantagem", aponta.

Bruno Castro confessa que há, no entanto, muitas empresas que arriscam porque têm os negócios parados e pagam a verba exigida pelos "hackers".

Quando são alvos de ataque informático, as empresas apresentam queixas às autoridades. O mesmo fez a EDP, depois do mais recente ataque, mas este especialista, habituado a perícias judiciais informáticas, afirma que "acaba por cair numa queixa contra desconhecidos" e, muitas vezes, sem grande sucesso.

"São sistemas maduros e é difícil chegar ao autor ou organização que fez o ataque. Há acções de investigação a posteriori ou no decorrer da acção do crime, mas é muito difícil", diz.

"No mundo cibernauta, não há geografias e os ataques são dispersos pelos IP, vão rolando porque todos vivemos no mesmo mundo da internet."

Ataques com "imenso sucesso"

O "phishing" é, nesta altura, um crime muito praticado. Garante Bruno Castro que só neste primeiro trimestre do ano já teve em mãos mais casos do que na última metade do ano passado - destas e outras acções informáticas ilícitas.

"Enviar algo de interesse para a pessoa até ela clicar, um tema atractivo. Quando a pessoa cai no erro, podem acontecer inúmeras coisas: activação de vídeos, passagem a outro site falso onde se introduzem dados e acessos ao homebanking", alerta.

Mensagens e e-mails fraudulentos tentam arrancar um simples "click "que abre portas à devassa de toda a privacidade.

A Pandemia de Covid -19 tem sido um "isco universal".

"Dizer que as análises são positivas ou que há uma aplicação que mostra a propagação da pandemia e somos prontamente empurrados a clicar, ou a descarregar uma aplicação, e depois instalam-se vídeos, roubam-se dados, passwords dos computadores ou do telemóvel. Roubam-se dados, dinheiro, etc... Isto tem sido uma prática massiva neste momento", diz Brun Castro.

Desafio às empresas

"Todos vivemos na internet, quer queiramos quer não, e o tecido empresarial colocou a estrutura humana a trabalhar fora, como se estivesse no escritório ou fábrica, em teletrabalho."

Esta realidade levanta desafios: primeiro, conseguir colocar trabalhadores com total acesso às plataformas para conseguirem trabalhar normalmente. Segundo, não colocar a segurança da empresa em causa uma vez que há milhares de ligações externas com internet doméstica. É preciso, por isso, muito mais cuidado.

Ataques informáticos: o que querem?

Um ataque não passa só por roubar informação, mas também por usurpar identidades. "Aceder a um email de um administrador ou politico permite falar por ele, dar ordens de pagamento. Todos estamos em teletrabalho e pouco se desconfia de determinadas coisas. Não nos cruzamos, como habitualmente, com as pessoas no corredor e não questionamos determinados actos", revela.

Usurpação de identidade e roubo do email são crimes que se têm registado de forma frequente nesta fase pandemia,admite este especialista em cibercrime.

"Há empresas com nível de maturidade baixa, onde se fazem transferências que não se detectam. É fácil enganá-las porque não estão habituadas a trabalhar com o virtual, na internet, e este novo paradigma do email, tudo isto faz com que detectem o esquema apenas após 3 ou 4 transferências bancárias já realizadas e impossíveis de recuperar. Por vezes detectam-se um mês ou mais depois", conta

Os ataques são cirúrgicos e sabem bem o que procuram. "Se quiserem, por exemplo, atacar um politico de renome, procuram fotografias e mensagens pessoais. Numa empresa, por seu lado, querem informações de negócios duvidosos ou de verbas avultadas", exemplifica Bruno Castro.

"O email é uma fonte de informação altamente relevante, tem volume massivo de informação num só sistema e este é o primeiro ponto de ataque."

O que estão a fazer as empresas para melhorar a segurança das informações e dos clientes?

A GALP diz que "a segurança é um dos pilares da cultura da empresa e isso é tão válido no mundo físico, como no mundo cibernético".

A empresa diz que é "continuamente alvo de tentativas de ataques cibernéticos", tendo em permanência uma equipa de reacção com ferramentas digitais "para monitorizar e dar resposta a incidentes cibernéticos".

Neste período de pandemia, a empresa tem observado um conjunto de ciberataques mais especificamente focados na temática do COVID-19.

Assim, tem apostado "na prevenção, nomeadamente, através de formação e informação prestadas aos colaboradores".

A utilização dos serviços online, "que permitem gerir contratos de eletricidade e gás ou solicitar entregas de gás engarrafado, teve um acréscimo de atividade que anda na ordem dos 50% em vários serviços".

A Altice não tem "até ao momento, registo de qualquer ataque. Dispõe de "um centro de cibersegurança que atua 24 horas por dia, com vista a prever e prevenir possíveis ataques".

Admite, no entanto, que já foi veiculo "aproveitado por um elevado número de agentes de ciberameaças como cobertura para as suas campanhas de ciberataques". Por isso, realizou uma mudança de paradigma na forma como as atividades profissionais e pessoais são realizadas. A Altice Portugal tem mais de 10 mil trabalhadores em teletrabalho.

A operadora de telecomunicações NOS argumenta que “a segurança da informação dos clientes é crítica pelo que fez um forte investimento nesta área". A empresa monitoriza permanentemente a rede que, para já, não foi alvo de qualquer ataque.

Em resposta à **Renascença**, a Procuradoria Geral da Republica revela que ainda não tem os dados quantificados, mas que no decurso deste período de pandemia tem-se verificado um aumento dos fenómenos de cibercriminalidade. Mensagens fraudulentas e emails são os principais veículos.

"O facto de haver milhões de pessoas em casa, em teletrabalho, utilizando meios de comunicação à distância e acesso remoto a sistemas informáticos, tem sido detetado um número muito significativo de mensagens fraudulentas que veiculam a prática de cibercrimes. Designadamente, assim acontece com mensagens de email e SMS contendo malware (por exemplo software de ransomware). Noutros casos, igualmente muito numerosos (também email ou SMS), as mensagens contêm links para páginas de phishing’, explica.